CONTINUATION IN SUPPORT OF SEARCH WARRANT

I, Brad Gittus, hereby depose and state as follows:

1. I make this continuation in support of an application for a warrant to arrest JACOB PHILLIPS, date of birth 04/08/1994, and to search (i) a residence located at 17219 McPhail Ave. NE, Cedar Springs, MI 49319 (the "Subject Premises"); and (ii) the person of JACOB PHILLIPS —each further described in Attachment A—to seize and analyze evidence, instrumentalities, or contraband related to criminal violations of 18 U.S.C. § 2252A, as further described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations assigned to the Office of the Resident Agent in Charge, Grand Rapids, MI. I have been so employed since September 2015. In 2016, I graduated from the Criminal Investigator Training Program and Homeland Security Special Agent training at the Federal Law Enforcement Training Center. While there I received specific training on cybercrimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. § 2252A, which forbids knowingly receiving or distributing child pornography, as defined in 18 U.S.C. Section § 2256(8).

3. I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children. In addition, I have been involved in and conducted numerous investigations regarding child pornography and exploitation, including by (i) participating in searches and seizures of computers and digital media; (ii) arresting and interviewing subjects; and (iii) forensically examining digital evidence.

4. This continuation is based on information I personally obtained, as well as information I received from other investigators participating in this investigation. This Continuation is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. Based on my training and experience, and the facts set forth herein, I believe there is probable cause that JACOB PHILLIPS committed crimes in violation of 18 U.S.C. § 2252A, and also that the Subject Premises and JACOB PHILLIPS, both further described in Attachment A, contain or have evidence, instrumentalities, or contraband related to these crimes, as further described in Attachment B.

PERTINENT STATUTE

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A. Section 2252A(a)(2) prohibits knowingly distributing any child pornography using any means or facility of interstate commerce.

BACKGROUND AND PROBABLE CAUSE

7. In August 2023, a federal agent working undercover (the "UC") accessed a secure, end-to-end encrypted online chat platform known as Kik Messenger. While logged onto Kik Messenger, the UC saw that a user identified as "john.star0100" (herein "JOHNSTAR"), within a chat room labeled "#lol.4iloveit," posted the statement: "29 male Michigan usa Father of a daughter as well."

8. In August 2023, the UC observed JOHNSTAR post a 37 second video file depicting a nude prepubescent female lying on her back in a bathtub, with her legs raised above her head. The prepubescent female is wearing a mask and her genitals are displayed. An adult male's penis can be seen, and he appears to urinate on the prepubescent female. The UC then initiated a private chat with JOHNSTAR on Kik.

9. During the chat, JOHNSTAR stated that he was a father of a 5-year-old girl and that he was the most sexually attracted to 3-year-olds. When the UC asked if he had "done anything with them?", JOHNSTAR replied "Yes starred [sic] to in the last year." JOHNSTAR then sent two image files depicting the same prepubescent female in various stages of undress.

10. When asked if he had any sexual contact with the girl, JOHNSTAR replied, "Anal And jerked." JOHNSTAR later explained his necessity to be discreet while on Kik because the girl was his "real daughter."

11. JOHNSTAR sent the UC several images and videos depicting various children being sexually abused. The UC sent these files to the National Center for Missing and Exploited Children ("NCMEC"), which confirmed that these were images and videos known to NCMEC and that they contain child pornography as defined under federal law because they depict "a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8)(A). I have also reviewed the videos and images and confirmed that they appeared to be child pornography, for instance:

a. Several of the videos depicted minor and prepubescent females being sexually penetrated by adults.
b. One video depicted a female child who appeared to be a toddler. The child was being anally penetrated by an adult female with an artificial penis.
c. Another video depicted another female toddler being vaginally penetrated by an adult male's penis.
d. Additionally, at least one video was from the known "Vicky" series, a well-known series in the child pornography realm that depict a minor girl being repeatedly sexually abused by her father.

12. In August 2023, JOHNSTAR sent the UC an image depicting a minor female asleep on a bed. The minor female appeared to be 4 to 6 years old, and her hand is positioned next to an adult male's penis. The male's face is not visible in the image. This image was unknown to NCMEC, indicating that this was possibly a newly produced image.

13. Kik Messenger operates by allowing users to send communications over the internet or cellular telephone service. The internet and telephone are both means and facilities of interstate commerce.

14. In August 2023, federal investigators obtained subscriber information and internet protocol address ("IP") logs associated with JOHNSTAR's account from Kik. Here is a summary of what investigators obtained:

> **Email:** john.star8900@gmail.com
> **IP history associated with Verizon Wireless:**
> August 3, 2023: 174.210.199.181 and
> 2600:1007:b117:78c7:8500:d384:62f3:73d8
> August 9, 2023: 174.240.112.90
> August 11, 2023: 174.240.112.77
>
> **IP history associated with Charter Communications:**
> August 9, 2023: 47.225.181.92
>
> **IP history associated with Point Broadband Fiber Holding:**
> August 23, 2023: 69.36.63.55

15. Through law enforcement database checks, federal investigators confirmed that the IPs 174.210.199.181, 2600:1007:b117:78c7:8500:d384:62f3:73d8, 174.240.112.90 and 174.240.112.77 are associated with the Verizon Wireless telephone number (616) 446-7863 (herein "**Target Phone**").

16. In August 2023, federal investigators obtained subscriber information and IP logs associated with the john.star8900@gmail.com account from Google. Here is a summary of what investigators obtained:

> **Account Creation Date:** 8/03/2023
> **Account Creation IP:** 2600:1007:b117:78c7:8500:d384:62f3:73d8

17. In August 2023, federal investigators obtained subscriber information associated with IP 47.225.181.92 from Charter Communications. Here is a summary of what investigators obtained:

Full Name: Tobie Phillips
Address: 184 South Union St. Sparta, MI
Country/Zip Code: 49345
Phone Number: (616) 446-1458

18. Through open-source internet research and law enforcement database checks, investigators confirmed the address of 184 South Union St. Sparta, MI 49345 to be associated with JACOB PHILLIPS in addition to Tobie Phillips. This research also revealed that Tobie Phillips is the father of JACOB PHILLIPS.

19. Through open-source internet research and law enforcement database checks, investigators obtained several reports from the Kent County Sheriff's Office as well as Kent County Child Protective Services ("CPS"). In each of these reports JACOB PHILLIPS's telephone number is listed as the **Target Phone**.

20. The records from August 12, 2023, show that JACOB PHILLIPS previously lived with his father at 184 South Union St. Sparta, MI 49345 but that he no longer lived at the residence after he and his father had a domestic altercation.

21. After that time, no additional IP addresses from the JOHNSTAR Kik messenger chats came back to 184 South Union St. Sparta, MI 49345. Many of the IP addresses associated with the JOHNSTAR account after that point were linked to 17219 McPhail Ave. NE Cedar Springs, MI 49319 ("Subject Premises").

22. The records also revealed that JACOB PHILLIPS was previously in a romantic relationship with "Whitney S Medwayosh" and they had a child together. A search of Whitney S Medwayosh's social media accounts revealed an Instagram account under the name "Whitney S Medwayosh" with "Mother of [Minor Victim] August 30th, 2018" listed as the user descriptions.[1]

23. The social media search also revealed a Facebook account in Whitney S Medwayosh's name. There were multiple pictures of a young girl posted on the account. The young girl appeared to be the girl in the image that JOHNSTAR previously sent that depicted the girl asleep next to an adult male's penis.

[1] The Minor Victim's name is known to law enforcement and can be provided to the judicial officer upon request.

24. In September 2023, federal investigators obtained an investigative report prepared the Kent County Child Protective Services ("CPS"). This report details a January 2023 encounter with JACOB PHILLIPS and Whitney S Medwayosh concerning the welfare of their daughter. The CPS investigator conducted a follow-up phone call to the **Target Phone**. The investigator stated that JACOB PHILLIPS answered the phone and verified his identity by confirming his date of birth.

25. In September 2023, federal investigators obtained updated subscriber information associated with JOHNSTAR from Kik. Here is a summary of what investigators obtained:

IP history associated with Point Broadband Fiber Holding:
September 4, 2023: 69.36.59.100
September 5, 2023: 69.36.59.100
September 6, 2023: 173.225.193.75

IP history associated with Charter Communications:
September 5, 2023: 47.224.42.94
September 5, 2023: 71.82.177.6

26. In September 2023, federal investigators obtained subscriber information associated with 69.36.59.100 and 173.225.193.75 from Point Broadband Fiber Holding. Here is a summary of what investigators obtained in relation to 69.36.59.100:

Full Name: Matthew Phillips
Address: 17219 McPhail Ave. NE Cedar Springs, MI 49319 ("Subject Premises")
Email Address: matthewph042@gmail.com
Phone Number: (616) 490-6490

Here is a summary of what investigators obtained in relation to 173.225.193.75:

Full Name: Fred Nix
Address: 19207 Jefferson Rd, Morley, MI 49336

27. Through law enforcement database checks, investigators confirmed that Matthew Phillips is the brother of JACOB PHILLIPS and owns the house located at Subject Premises.

28. In September 2023, federal investigators obtained updated subscriber information associated with the IPs 47.224.42.94 and 71.82.177.6. Here is a summary of what investigators obtained in relation to 47.224.42.94:

Subscriber Name: Hart Enterprises
Address: 400 Apple Jack Ct, Sparta, MI 49345

Here is a summary of what investigators obtained in relation to 71.82.177.6:

Subscriber Name: DSR MCD 7479
Address: 450 W Division St, National Account, Sparta, MI 49345

29. Through open-source internet research and law enforcement database checks, investigators confirmed that JACOB PHILLIPS is employed by Hart Enterprises located at 400 Apple Jack Ct, Sparta, MI 49345. Investigators also confirmed the address of 450 W Division St, National Account, Sparta, MI 49345 to be a McDonalds restaurant located adjacent to Hart Enterprises.

30. I reviewed the image depicting a minor female appearing to be 4 to 6 years old with her hand is positioned next to an adult male's penis. I compared this image to the images recovered from Whitney S Medwayosh's social media and believe the girl depicted in this photo to be the biological daughter of JACOB PHILLIPS and Whitney S Medwayosh.

31. One day in September 2023, federal investigators observed a tan Chevrolet Tahoe, bearing MI license plate ESS1703 parked at the Subject Premises. Michigan Secretary of State records confirm this vehicle is registered to JACOB PHILLIPS. A silver Jeep Grand Cherokee, bearing MI license plate ENE3149, was also observed at the Subject Premises. Michigan Secretary of State records confirm this vehicle is registered to Matthew Phillips.

32. On September 20, 2023, law enforcement observed the Tahoe parked at the Subject Premises for at least two hours, and I am aware that the Tahoe is currently parked at the residence.

33. I submit there is probable cause to believe that JACOB PHILLIPS distributed child pornography in violation of 18 U.S.C. § 2252A(a)(2) and that the Subject Premises and JACOB PHILLIPS contain or have evidence, instrumentalities, or contraband related to this crime.

34. I respectfully request that this Court issue a warrant for PHILLIPS's arrest on this charge and an order to seal this criminal complaint and warrant. I further request a warrant to search the Subject Premises and JACOB PHILLIPS, both further described in Attachment A, for evidence, instrumentalities, and contraband related to this crime, as further described in Attachment B.

CHARACTERISTICS OF PEOPLE WITH AN INTEREST IN CHILD PORNOGRAPHY

35. Based on my training and experience, characteristics common to people with an interest in child pornography include that they:

a. Generally have a sexual interest in children and receive sexual gratification viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including in hard copy and/or digital formats. Child pornography viewers and collectors oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sex, or to demonstrate the desired sexual acts. They may also use toys, games, costumes, sexual clothing, sexual paraphernalia, and children's clothing to lure or entice children. They may keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

c. May take photographs that either constitute child pornography or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such images and video may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

d. Generally maintain their collections in a safe, secure, and private environment, most often where they live and/or on their person. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based

chat messaging, email, text message, video streaming, letters, telephone, and in person.

SPECIFICS PERTINENT TO SEARCHING COMPUTERS

36. Based on my training and experience, I know the following:

a. People who use electronic devices to produce, possess, and distribute child pornography often amass vast collections of such material, and use multiple different devices to obtain and store it.

b. Computers and other internet capable devices such as tablets and cellular telephones facilitate the collection and distribution of child pornography.

c. People involved in sexual exploitation of children generally maintain their collections in a safe, secure, and private environment, most often where they live and/or on their person. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the residence or by anyone else who enters the home. Such hiding places could include but are not limited to garages, sheds, attics, vehicles, bags, and pockets. Digital files and devices may be password protected, encrypted, or otherwise protected.

d. The internet, including online chats platforms like Kik, is commonly used as means and facility of interstate commerce, and it affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and seemingly-anonymous manner.

e. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage media that contains thousands of files, including images, video files, and full length movie files.

f. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider client software, among others. In addition to electronic communications, a computer user's internet activities generally leave traces in a computer's web cache and internet history files.

g. A forensic examiner often can recover evidence that shows whether a computer device contains peer to peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that date remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

h. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

i. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

i. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal

criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on site.

ii. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

j. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

k. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize not only the digital storage media and to search it for evidence in the form of child pornography images or videos, stored emails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with collectors of child pornography or with actual children, but also requests permission to seize all hardware, software, and computer security devices necessary to access and examine the computer storage media. Peripheral equipment including printers, routers, modems, network equipment used to connect to the Internet may also contain evidence of what devices were used to connect to the Internet, who used those devices, and what actions the person(s) performed while using such devices.

l. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

m. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain.

SEARCH PROTOCOL

37. Investigators plan to search the Subject Premises and Subject Person for any material described in Attachment B.

38. The government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

REQUEST FOR AUTHORIZATION TO UNLOCK DEVICES

39. Based on my knowledge and experience, and information provided to me by others, I know that certain electronic devices may be locked and/or unlocked by personal identification numbers ("PIN"), gestures or motions, and/or with biometric features, such as thumb and fingerprint recognition (collectively, "fingerprint ID") and/or facial recognition ("facial ID").

40. If a user enables the fingerprint ID unlock feature on a device, he or she can register several fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's sensor, which typically is found on the front of the device. In my training and experience, users of devices that offer fingerprint ID or facial ID often enable it because it is considered to be a more convenient way to unlock the device than by

entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

41. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. Depending on the configuration of the security settings on the phone, the opportunity to unlock the device via fingerprint ID or facial ID exists only for a short time. Fingerprint ID and facial ID also may not unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) several unsuccessful attempts to unlock the device are made.

42. The passcode or password that would unlock the device(s) is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) or present the face of the user(s) of the device(s) found during the search to the device's fingerprint ID or facial ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via fingerprint ID or facial ID is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

43. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s), this will result in the device requiring the entry of a password or passcode before it can be unlocked.

44. Based on the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of PHILLIPS to the fingerprint ID sensor or to present his face to the facial ID sensor of any seized device(s) to attempt to unlock any devices seized under this warrant in order to search their contents as authorized by this warrant.